

UNITED STATES DISTRICT COURT

for the
District of Oregon **FILED 29 JAN '18 11:20 USDC-ORP**

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Apple iPhone FCC ID: BCG-E2816A, EC:579C- E2816A,
IMEI: 356984066839841

Case No. **'18-MC- 65**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Apple iPhone FCC ID: BCG-E2816A, EC:579C- E2816A, IMEI: 356984066839841 described in Attachment A hereto,

located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2113(a)

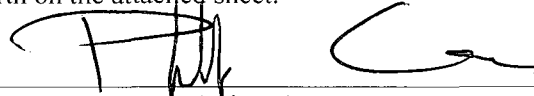
Bank Robbery

Offense Description

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Phillip Garcia, Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: Jan. 29, 2018



Judge's signature

City and state: Portland, Oregon

Stacie F. Beckerman, United States Magistrate Judge

Printed name and title

ATTACHMENT A

Description of items to be searched.

The phone to be searched is an gray Apple Iphone FCC ID: BCG-E2816A, EC:579C-E2816A, IMEI: 356984066839841, currently located on the premises of the FBI Portland Office located at 9109 NE Cascades Pkwy, Portland, Oregon, 97220.

ATTACHMENT B

Items to Be Seized

All records on the Device described in Attachment A that relate to violations of Title 18, United States Code 2113(a), and involved Deante Von Gibson, including:

1. Records, Documents, and Visual Depictions:

- a. Web sites visited, to include originating Internet Protocol (IP) address:
- b. Images of Deante Von Gibson, and any data associated with such images, including metadata concerning the date, time, and location the images were taken, and the device(s) the images were taken with;
- c. Images of cities or locations in the state of Oregon and Washington, and any data associated with such images, including metadata concerning the date, time, and location the images were taken, and the device(s) they were taken with.
- d. Internet search history and temporary internet files
- e. Call history for the Apple Iphone described in Attachment A, including lists of numbers dialed, calls received, and the dates, times, and duration of calls made or received; caller identification information for numbers dialed or calls received, stored text messages sent or received, to include those sent via mobile chat apps and messaging services, and the dates and times those messages were sent or received; and the contents of any directories or contact lists stored in the devices.
- f. Any stored GPS location information to include searches made, saved favorite locations, and any time the GPS features of the devices stored physical information, to the phone or within any other application.

g. Any appointments or dates saved in the calendar or other applications or means of saving dates or reminders.

h. Documents which reveal or suggest who possessed or used the devices described in Attachment A and or/ where they were physically located when they device was used.

i. Record of Internet Protocol (IP) addresses used by the device listed in Attachment A;

j. Records of Internet Activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

k. Any records of internet usage, including records containing screen names, user names, logon information, e-mail addresses, and identifies assumed for the purposes of communication on the Internet. Such records include billing and subscriber records, chat room logs, and e-mail messages, and include electronic files in a computer or on data storage media.

As used above, the term “records, “documents,” “programs,” “applications,” or “materials” includes records, documents, programs, applications, or materials created, modified, or stored in any form.

2. Digital Evidence:

- a. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the digital device;
- b. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device;
- c. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices, including the web browser's history; temporary Internet files; cookies; bookmarked or favorite web pages; email addresses used from the device; Internet Protocol addresses used by the device; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. Search Procedure

- a. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

b. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

c. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

d. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

e. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the

data contained therein.

f. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF Phillip Garcia

**Affidavit in Support of an Application
for a Search Warrant for a Phone**

I, Phillip Garcia, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation (“FBI”) and have been since March 2017. I am currently assigned to the Portland Division of the FBI as part of the Violent Crimes Unit, and investigate violations of federal law including bank robberies in violation of Title 18, United States Code (“U.S.C.”), Section 2113(a). Prior to joining the FBI, I worked for approximately six years as a police officer with the Dallas, Texas and Grand Prairie, Texas Police Departments.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of an Apple iPhone cellular (or “wireless”) telephone bearing IMEI 356984066839841 (hereinafter “Phone”), which is currently in law enforcement custody at 9109 NE Cascades Parkway, Portland, Oregon, as described in Attachment A hereto, and the extraction of electronically stored information from the Phone, as described in Attachment B hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence contraband and instrumentalities of violations of 18 U.S.C. § 2113(a).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement

officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 18, United States Code, Section 2311(a) prohibits: “whoever, by force and violence, or by intimidation, takes or attempts to take, from the person or presence of another, or obtains or attempts to obtain by extortion of any property or money or any other thing of value belonging to, or in the care, custody, control, management, or possession of, any bank, credit union, or any savings and loan association[.]” 18 U.S.C. § 2113(a).

Statement of Probable Cause

5. On September 27, 2017, a robbery occurred at the Umpqua Bank located at 25529 SW Gwen Dr., in the City of Wilsonville, Clackamas County, Oregon (“the bank”). The bank, whose deposits were insured by the Federal Deposit Insurance Corporation (“FDIC”), suffered a loss of approximately \$3,293 in United States currency.

6. On September 27, 2017, at approximately 1:00 p.m., an unidentified black male carrying a blue Nike duffel bag (“the robber”) entered the bank, approached a bank teller (“Victim Teller 1”) and said, “I really need the money, they have my kids” while handing Victim Teller 1 a handwritten note that appeared to be written by a third party to the robber demanding \$100,000. Victim Teller 1 turned over \$2,116.00 from her till and showed the note to a nearby bank teller (“Victim Teller 2”). Victim Teller 2 read the note and surrendered an additional \$1,177.00 from her drawer. The robber placed the money into his blue Nike duffel bag.

7. The robber then exited the bank and got into the back seat of a black Honda Civic displaying Uber and Lyft stickers in the rear window and bearing Oregon plate number 438HYK.

8. Bank employees described the robber as a thin black male, approximately 6'0, dressed in a black t-shirt with white stripes, wearing big round sunglasses with dark purple lenses that were described as almost "feminine."

9. Investigators located the telephone number for the registered owner of the black Honda Civic ("the driver") and made contact with him. The driver told investigators that he is a commercial driver for Uber and had recently given a male a ride to the Umpqua Bank in Wilsonville, Oregon. Upon learning that a bank robbery had occurred at Umpqua Bank while the driver was parked outside, the driver told investigators that approximately 45 minutes prior to arriving at Umpqua Bank, he was flagged down by an unknown male near SW Pine Street and Third Avenue in downtown Portland. The male identified himself as Deante and asked to be driven around town so he could finish a couple of errands. Deante told the driver that he would pay cash for the services.

10. On their way to Umpqua Bank, the driver covertly took a photograph of Deante as a precautionary measure. Once they arrived at Umpqua Bank, Deante entered the bank carrying a blue Nike duffel bag. The driver described the encounter as "odd." After a few minutes, Deante exited the bank and paid the driver \$100 in twenty dollar denominations.

11. After leaving the bank, the driver took Deante to the area near 20th and Burnside Street because Deante said he needed to wire some money through Western Union. The driver told investigators that he was "almost sure" Deante went into Fred Meyer.

12. Officers with the Portland Police Bureau and the FBI responded to the Fred Meyer located at 100 NW 20th Place, Portland, Oregon, but were unable to locate the robber. Inside a

restroom however, officers found a blue Nike duffel bag which appeared to have been discarded.

Inside the bag was a book autographed to “DEANTE”, a pair of dark sunglasses, a gray sweatshirt, a barber’s cape, several pairs of barber clippers, a pair of leather gloves, business cards, and a piece of paper with the name DEANTE VON GIBSON. A law enforcement database check located a Deante Von Gibson, with an Oregon driver’s license and prior criminal history in Texas.

13. On November 13, 2017, Special Agent Garcia submitted an affidavit in support of a criminal complaint and arrest warrant which was reviewed by Assistant United States Attorney John Brassell and signed by United States Magistrate Judge Paul J. Papak. The criminal complaint authorized an arrest warrant on Deante Von Gibson for one county of bank robbery in violation of Title 18, United States Code, Section 2113(a).

14. On December 28, 2017, the Fort Bend County Constable’s Office contacted Deante Von Gibson during a traffic stop in the 24500 block of Cinco Ranch Blvd., Katy, Fort Bend County, Texas. Deante was arrested on the federal warrant, and during a search incident to arrest, officers seized an Apple I-phone, IMEI number 356984066839841, in a gray case. After examining the seized phone, it appears to match the physical description of the phone used by Deante in the photograph taken by the Uber driver.

Information Regarding the Devices

15. The Phone is currently in the lawful possession of the FBI. It came into the FBI’s possession in the after it was seized incident to arrest by the Fort Bend County Constable’s Office.

16. The Phone is currently in storage at 9109 NE Cascades Parkway, Portland, Oregon. In my training and experience, I know that the Phone has been stored in a manner in

which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Phone first came into the possession of the FBI.

17. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet,¹ including the use of apps.² Wireless telephones may also include a global positioning system (“GPS”) technology for determining the location of the device.

18. Based on my training, experience, and research, I know that the Phone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, etc. In my training and experience, examining data stored on wireless

¹ The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

² Apps is an abbreviation for applications. An app is a self-contained program or piece of software designed to fulfill a particular purpose. An app can run on the Internet, on a computer, on a cell phone, or on other electronic devices.

telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

19. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Phone because, based on my knowledge, training, and experience, I know:

a. Phones can store information for long periods of time, including information viewed via the Internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, the Phone may contain electronic evidence of how it has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes

automatically downloaded into a temporary Internet directory or “cache.”

d. Data on the Phone can provide evidence of a file that was once on the Phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Phone that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the Phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times the Phone was in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

f. A person with appropriate familiarity with how the Phone works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Phone was used, the purpose of its use, who used it, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Phone is evidence may depend on other information stored on the Phone and the application of knowledge about how a Phone functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how the Phone was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the Phone.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Phone consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Phone and computer-assisted scans and searches of the entire Phone that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

21. The initial examination of the Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

22. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the

warrant, through the conclusion of the case.

23. If an examination is conducted, and it is determined that the Phone does not contain any data falling within the ambit of the warrant, the government will return the Phone to its owner within a reasonable period of time following the search and will seal any image of the Phone, absent further authorization from the Court.

24. The government may retain the Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phone and/or the data contained therein.

25. The government will retain a forensic image of the Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.


26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

27. Based on the foregoing, I have probable cause to believe, and I do believe, that the Phone described in Attachment A contains evidence, contraband, and instrumentalities of violations of Title 18 U.S.C. § 2113(a), as set forth in Attachment B. I therefore request that the

Court issue a warrant authorizing a search of the Phone described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

28. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) John Brassell and advised me that in his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.



Phillip Garcia
Special Agent, FBI

Subscribed and sworn to before me this 29th day of January 2018.



STACIE F. BECKERMAN
United States Magistrate Judge